Guida rapida all'utilizzo di eXtensiveControl®

Table of Contents

Guida rapida all'utilizzo di eXtensiveControl

Aprile 2010

Informazioni di servizio e di supporto

Versione del prodotto

Questo guida rapida si riferisce al programma eXtensiveControl® versione 1.x. Per ottenere supporto tecnico, servizi per l'utente e informazioni sulla vendita del prodotto è possibile utilizzare l'indirizzo riportato in seguito.

Telefono

Supporto tecnico e commerciale:

+39 (0)521 708811

Il supporto telefonico è fornito nei giorni feriali dalle 8:30 alle 12:30 e dalle 14:30 alle 18:30 (ora locale)

È necessario un contratto di supporto.

WEB

http://www.symbolic.it

Posta elettronica

Supporto tecnico: <support@symbolic.it>

Vendite: <sales@symbolic.it>

Indirizzo di posta

Symbolic S.p.A.
Viale Mentana, 29
CAP 43100 Parma
Italy

Capitolo 1. Introduzione

Questa breve guida ha lo scopo di illustrare le caratteristiche principali del prodotto e di permetterne l'utilizzo nel più breve tempo possibile, almeno per quello che riguarda le configurazioni e gli scenari più comuni.

Installazione

Il prodotto viene distribuito sia su supporto ottico (*CDROM*) sia via WEB. In entrambi i casi per installare eXtensiveControl® è sufficiente eseguire il file Setup.exe (nel caso si stia utilizzando il CD e sia attivo l'autorun di Windows, verrà presentata una interfaccia che permette di iniziare l'installazione).

Attenzione: se si effettua l'installazione da CD, si consiglia di controllare, tramite il tasto "*Verifica sul WEB disponibilità nuova versione*" sul menù del CD, se vi è una nuova versione disponibile, dal momento che il CD per ovvie ragioni potrebbe non essere aggiornato alla ultimo build disponibile del prodotto. A tal proposito sul menu del CD è possibile visualizzare la release (quattro numeri in basso a sinistra rispetto al logo) del package e confrontarla con quella del sito Symbolic per decidere se scaricarlo.

Sul CD di installazione sono inoltre presenti le versioni in prova (trial) di 30 giorni dei prodotti F−Secure Anti−Virus per server e workstation. Se si desidera utilizzare uno dei due prodotti per effettuare la scansione antivirus è consigliabile installare prima l'antivirus e poi il prodotto in modo che il wizard di installazione di eXtensiveControl® sia in grado di rilevare la presenza dell antivirus e autoconfigurarsi di conseguenza. Il menù principale del CD provvede a rilevare se il sistema operativo installato è un server o una workstation e presenta una opzione per avviare automaticamente l'installazione della versione corretta dell'antivirus (cioè server o workstation).

Prima dell'installazione sono da considerare i seguenti requisiti minimi:

- *Spazio su disco*: si consiglia di installare il prodotto su una partizione del disco fisso capiente poichè oltre ai file del prodotto stesso sarà necessario avere spazio per i file di log generati da eXtensiveControl®. Più spazio è disponibile su disco, meno frequentemente sarà necessario archiviare i file presenti nella cartella di log.
- *Risorse*: requisiti di sistema come potenza del processore e quantità di memoria dipendono dai moduli utilizzati e dal traffico che deve essere gestito. In particolare il filtro sulla posta richiede risorse che variano a seconda che sia attivo o meno il filtro antivirus e in questo caso dal tipo di messaggi (in particolare dalla dimensione degli allegati).
- *Codice del prodotto*: è necessario disporre di un codice definitivo per eXtensiveControl® ed un codice per SurfControl® nel caso si sia acquistato anche il suddetto plug−in. Se non di dispone del codice, l'installatore abiliterà il prodotto in modalità trial (30 giorni). È comunque possibile passare dalla modalità trial a quella definitiva in qualunque momento inserendo gli opportuni codici.
- *Porta di ascolto del configuratore*: eXtensiveControl® è configurabile attraverso l'uso di un browser. A questo scopo viene installato un server Web dedicato alla configurazione del prodotto. Per default questo server utilizza la porta 8000. Se questa porta dovesse risultare occupata è possibile al momento dell'installazione selezionarne un'altra.
- *Password di amministrazione*: durante l'installazione è necessario fornire al prodotto la password che sarà usata per amministrare eXtensiveControl®. Questa password è associata all'utente "Admin". Tale utente potrà poi in seguito creare altri account e abilitare l'accesso da altre macchine (vedere manuale).
- *Upgrade del prodotto*: se invece di una installazione *ex−novo* si sta effettuando un upgrade del prodotto, si consiglia di procedere all'aggiornamento *senza* disinstallare la vecchia versione. Il programma di installazione è in grado di riconoscere che vi è già una versione precedente installata e provvedere all'aggiornamento.

Funzionamento del prodotto

Al termine dell'installazione viene lanciato il wizard che permette di configurare velocemente il prodotto fornendo al programma i parametri di base che sono necessari al suo funzionamento. Il consiglio è quello di seguire passo passo le pagine presentate e solo in seguito, eventualmente, accedere al configuratore per modificare i parametri che il wizard non gestisce.

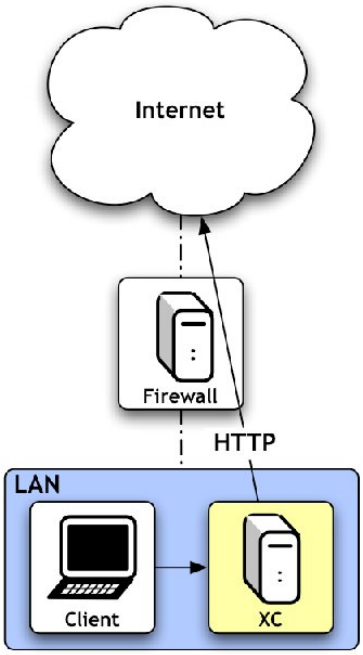
Seguono alcuni consigli e informazioni che possono risultare utili in fase di configurazione. Per un trattamento più approfondito si consiglia di consultare il manuale utente.

- *Struttura del wizard*: il wizard consente di impostare un eventuale collegamento con un dominio Active Directory, nonchè i parametri fondamentali per il modulo WEB, POP3, SMTP, ed MTA (Mail Transfer Agent) e di pianificare gli aggiornamenti dei database utilizzati da eXtensiveControl®.
- *Funzionamento come servizi*: ognuno di questi moduli funziona come servizio di Windows e parte (se attivato) automaticamente quando si avvia il computer nel quale il prodotto è installato. Non è necessario che ci siano utenti collegati alla macchina, tuttavia se ci sono, questi possono lavorare indisturbati (risorse della macchina permettendo) dal momento che ognuno di questi servizi agisce in background.
- *Filtro Web*: il modulo WEB consente di regolamentare la navigazione sul Web. È possibile permettere o vietare l'accesso a siti in base al loro contenuto, nome, file a cui si accede e le regole possono essere applicati a singoli computer o ad utenti. Per autenticare gli utenti utente è possibile usare come database un Workgroup, un dominio NT e un dominio Active Directory.
- *Filtro per la posta*: I moduli POP3 e SMTP gestiscono la posta elettronica e consentono di filtrare i messaggi di spam/phishing, mail contenenti malware (virus, trajan, ecc.) e imporre regole più complesse sui messaggi come ad esempio la dimensione massima degli allegati, i tipi di allegati, i tag contenuti negli header o nel body dei messaggi, ecc. Nel modulo SMTP è possibile filtrari i destinatari dei messaggi in base ad un filtro statico oppure, se si utilizza Exchange, in base alle informazioni contenute all'interno della struttura di Active Directory.
- *Antivirus*: il controllo antivirus sulla posta è subordinato alla presenza di un antivirus installato sulla macchina (che deve essere acquistato e installato a parte).
- *Indirizzi di bind*: per ogni modulo, ad eccezione dell'MTA (Mail Transfer Agent), occorre specificare un indirizzo e porta di ascolto. Tale indirizzo sarà quello che i vari client di posta e browser useranno per ottenere un servizio di filtraggio in base alle *policy* stabilite.
- *Configurazione del router/firewall*: al fine di permettere il corretto funzionamento del prodotto, sarà necessario configurare il router/firewall affinchè impedisca l'accesso diretto ai client a quelle particolari porte che consentono l'accesso diretto a servizi che si vuole invece filtrare. Ad esempio, se di decide di eliminare la categoria "Pornografia" dai siti WEB accessibili agli utenti, il browser dovrà essere configurato per accedere al modulo WEB, il quale filtrerà tali contenuti. Per evitare che utenti esperti superino il filtro uscendo direttamente senza passare da eXtensiveControl® è opportuno configurare il router/firewall per impedire l'accesso diretto alla navigazione da parte degli utenti.

Capitolo 2. Scenari di utilizzo di eXtensiveControl®

In questo capitolo verranno presentati alcuni scenari di esempio per l'utilizzo del prodotto. Ovviamente non vuole essere un insieme esaustivo di tutti i metodi di utilizzo ma solo un esempio dei modi in cui può essere impiegato.

Gestione della navigazione WEB

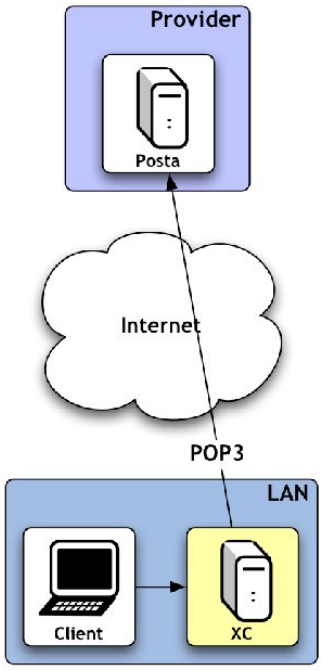


Un possibile impiego di eXtensiveControl® è quello di filtro della navigazione Web. In uno scenario applicativo di questo tipo il prodotto ha il compito di applicare una data politica aziendale sulla navigazione Internet. La policy potrebbe ad esempio inibire l'accesso a determinate categorie di siti, oppure discriminare l'accesso a Internet in funzione dell'orario, della macchina utilizzata, oppure dell'utente.

Questa funzione è implementata dal "Modulo WEB" di eXtensiveControl®, essa permette di ottimizzare le risorse aziendali.

eXtensiveControl® può essere installato su una qualunque macchina con un sistema operativo Windows in tecnologia NT raggiungibile da tutti gli host che devono navigare. Le macchine interne dovranno utilizzare eXtensiveControl® come proxy per la navigazione, quindi dovranno configurare il browser in modo opportuno. Come detto in precedenza, per evitare che gli utenti più esperti eliminino la configurazione del proxy uscendo direttamente verso Internet scavalcando eXtensiveControl®, è consigliabile impostare il firewall per impedire la navigazione da tutti i computer esclusa la macchina su cui è installato eXtensiveControl®. È consigliabile che la macchina abbia un indirizzo IP fisso per avere un riferimento fisso per le altre macchine. Ovviamente la macchina deve essere accesa per poter permettere la navigazione.

Gestione della posta con server di posta esterno



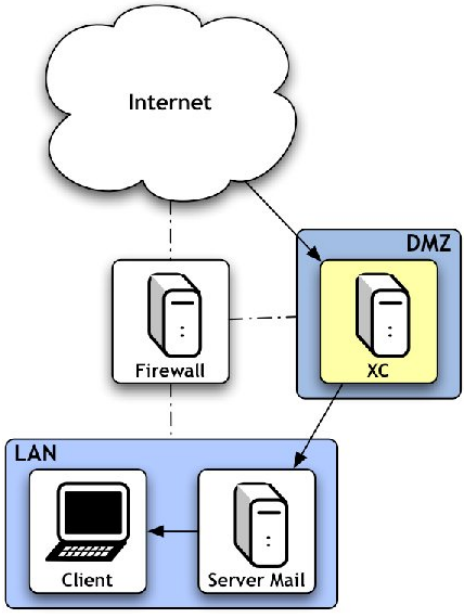
Un secondo possibile scenario di utilizzo di eXtensiveControl® è l'impiegaro per un controllo del contenuto della posta elettronica mediante il protocollo POP3. Si pensi ad uno studio professionale o comunque ad una piccola rete aziendale composta da poche macchine senza un server di posta interno in cui tutte le postazioni scaricano le proprie email mediante una connessione POP3 da un mail server esterno che spesso è quello del provider.

Il controllo offerto da eXtensiveControl® permette di verificare la presenza di malware all'interno dei messaggi, filtrare email di spam o di phishing ed email con determinati allegati o con determinate caratteristiche.

Anche in questo caso è necessario installare il prodotto su una qualunque macchina con un sistema operativo Windows in tecnologia NT raggiungibile da tutti quegli host che devono scaricare la posta elettronica. Le macchine interne dovranno utilizzare eXtensiveControl® come server POP3 (posta in ingresso), sarà compito di eXtensiveControl® contattare il mail server su cui si trova la casella di posta in questione. È possibile vincolare eXtensiveControl® per contattare sempre un determinato mail server (sicuramente la soluzione più semplice) oppure svincolarlo permettere agli utenti di specificare il server POP3 (in questo caso è possibile usare le ACL per gestire i server raggiungibili). Anche in questo caso per evitare che gli utenti più esperti eliminino la configurazione di eXtensiveControl® ed escano direttamente verso Internet, è consigliabile impostare il firewall per impedire ogni connessione in uscita esclusa la macchina su cui è installato eXtensiveControl®. È consigliabile che la macchina abbia un indirizzo IP fisso per avere un riferimento fisso per le altre macchine. Ovviamente la macchina deve essere accesa durante il download della posta.

In una configurazione di questo tipo tutto il traffico POP3 passerà attraverso eXtensiveControl®. Per essere esatti, il client di posta contatterà eXtensiveControl® per il download, il quale a sua volta si collegherà al mail server di riferimento. Sui messaggi di posta elettronica gestiti dal prodotto sarà possibile applicare un controllo AntiVirus, AntiSpam ed AntiPhishing, in più sarà possibile eseguire determinate azioni in funzione delle caratteristiche del messaggio stesso come mittente, destinatario, header del messaggio, allegati e molto altro. I messaggi ritenuti virati o comunque non sicuri vengono bloccati evitando che raggiungano il client.

Gestione della posta con server di posta interno



Un ulteriore scenario applicativo di eXtensiveControl® è l'utilizzo per il controllo della posta entrante in una rete aziendale mediante il protocollo SMTP. Un classico esempio è cosituito da una rete di medie dimensioni che presenta al suo interno un mail server per la gestione della posta aziendale.

eXtensiveControl® consente di analizzare in modo dettagliato tutte le mail che vengono inviate al mail server interno bloccando i messaggi indesiderati prima che questi raggiungano il mail server aziendale. Il controllo offerto permette di verificare la presenza di malware all'interno dei messaggi, filtrare email di spam o di phishing ed email con determinati allegati o con determinate caratteristiche.

Anche in questo caso è necessario installare il prodotto su una qualunque macchina con un sistema operativo Windows in tecnologia NT che possa raggiungere il mail server e sia raggiungibile dall'esterno. Bisognerà configurare la rete in modo che i messaggi provenienti dall'esterno non vengano inviati al mail server ma bensì a eXtensiveControl®, il quale dopo averli analizzati li invierà al mail server interno. È opportuno che la macchina abbia un indirizzo IP fisso per avere un riferimento per il forwarding dei messaggi. Ovviamente la macchina deve essere sempre accesa, in quanto le email potranno arrivare in un qualunque istante.

In una configurazione di questo tipo tutto il traffico di posta in ingresso passerà attraverso eXtensiveControl®. Ai messaggi di posta elettronica gestiti dal prodotto sarà possibile un controllo AntiVirus, AntiSpam ed AntiPhishing, in più sarà possibile eseguire determinate azioni in funzione delle caratteristiche del messaggio stesso come mittente, destinatario, header del messaggio, allegati e molto altro.

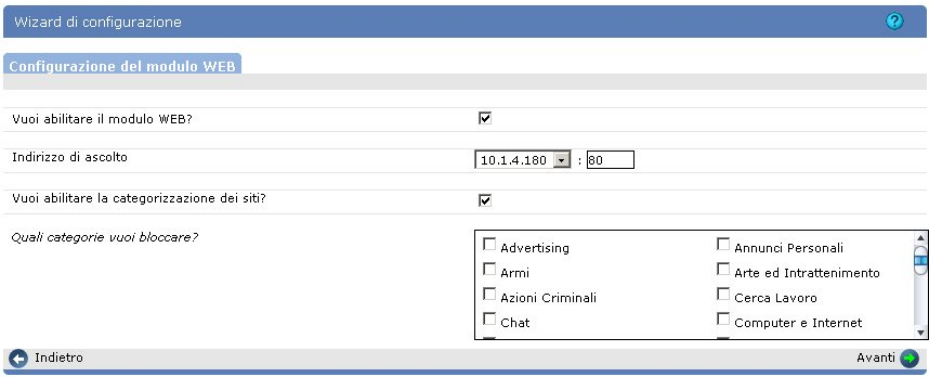
Capitolo 3. Configurazione del Modulo WEB

Come posso configurare il Modulo WEB per consentire la navigazione?

Il modo più semplice per configurare in modo generico il Modulo WEB affinchè consenti la navigazione è quello di usare il "Wizard di configurazione" subito dopo l'installazione di eXtensiveControl® (l'uso del Wizard cancella eventuali configurazioni già presenti).

1. Dalla schermata principale premere su "Wizard di configurazione" e poi autenticarsi con un utente avente i diritti di configurazione (ad esempio Admin).
2. Dalla schermata iniziale premere su Avanti.
3. Nella sezione dedicata al "Modulo WEB" selezionare "Vuoi abilitare il modulo WEB?" facendo apparire gli altri form di configurazione.

4. Indicare in "Indirizzo di ascolto" l'indirizzo IP e la porta su cui si porrà in ascolto il modulo. Si consiglia di mantenere i valori di default a meno che la coppia IP–porta non sia già in uso.

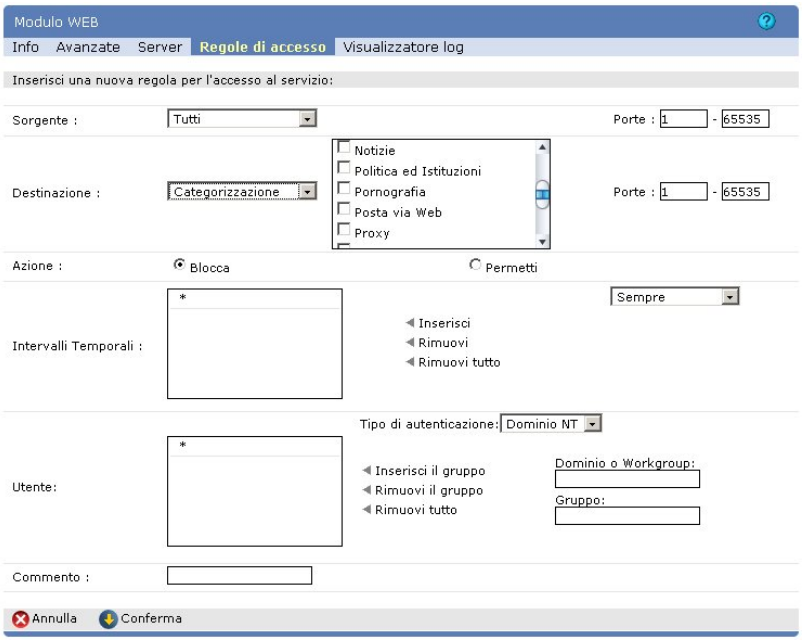


5. Qualora si volesse applicare subito la categorizzazione web selezionare "Vuoi abilitare la categorizzazione dei siti?" e poi scegliere i siti da bloccare nella finestra sottostante
6. Premere "Avanti" fino al completamento del Wizard e poi "Finito".
7. Come detto nella sezione scenari è consigliabile configurare il firewall per consentire la navigazione web solo dalla macchina su cui è installato eXtensiveControl® ed è necessario configurare tutti i browser per utilizzare eXtensiveControl® come proxy.

Come posso bloccare determinate categorie di siti?

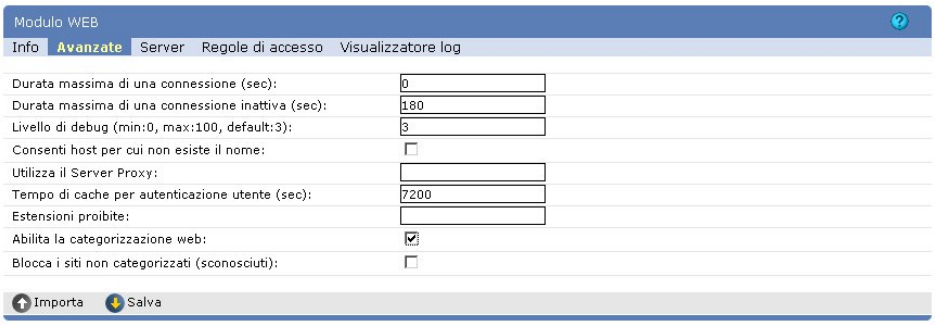
1. Dal configuratore premere su "Moduli" dal frame in alto e poi "Modulo WEB" dal menu sulla sinistra dell'interfaccia e poi "Regole di accesso" nella finestra principale.
2. Premere su "Rimuovi tutto" per cancellare la configurazione corrente ed iniziare la policy aziendale ex–novo. Confermare poi l'azione.

3. Premere su "Inserisci sopra" per inserire una nuova regola.
4. Nella nuova finestra, se si desidera applicare questo vincolo a tutti gli host locali lasciare nel campo "Sorgente" il valore "Tutti", altrimenti indicare mediante indirizzo IP o nome, le macchine a cui applicare questo vincolo. Nel campo "Destinazione" scegliere "Categorizzazione" e nella finestra che apparirà selezionare le categorie che si vogliono bloccare. Nel campo "Azione" mettere "Blocca". Premere poi su "Conferma".



5. Creare poi una regola in ultima posizione che permetta tutto. Premere su "Inserisci sotto", nella finestra di definizione scegliere l'azione "Permetti" lasciando tutti gli altri valori di default e poi premere Conferma. Le regole di accesso saranno:

6. Premere su Avanzate e selezionare la voce "Abilita la categorizzazione web", poi cliccare su Salva.

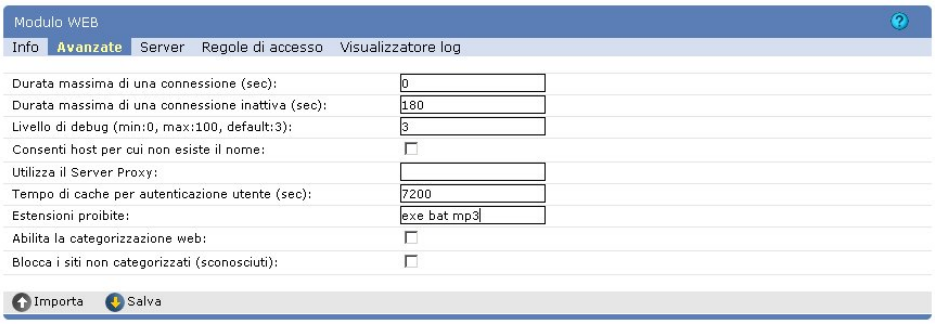


7. Prima di avviare il modulo WEB è necessario avere a disposizione il database di SurfControl® per poter categorizzare i siti in base al loro contenuto. Dal frame in alto premere su Sistema, poi dal menu a fianco su Categorizzatore WEB ed infine sulla sottosezione Avanzate.
8. Dalla voce Database di categorizzazione verificare che sia selezionato "SurfControl". Si ricorda che per utilizzare il database di SurfControl® è necessario un codice separato da quello del prodotto. Nella sezione SurfControl DB verificare che il database sia presente altrimenti provvedere al download premendo "Aggiorna ora" (il download può richiedere vari minuti in quanto la dimensione del database ` di circa 100MB).
9. A questo punto si può avviare/riavviare il Modulo WEB, andare su Moduli in alto, poi Modulo WEB a sinistra ed infine Info e riavviare il modulo.

Come posso impedire il download di file pericolosi?

1. Dal configuratore premere su Moduli in alto e poi Modulo WEB dal menu sulla sinistra dell'interfaccia e poi Avanzate nella finestra principale.

2. Inserire nella voce Estensioni proibite tutte le estensioni che devono essere bloccate separate da uno spazio (esempio: "exe mp3 bat ...").

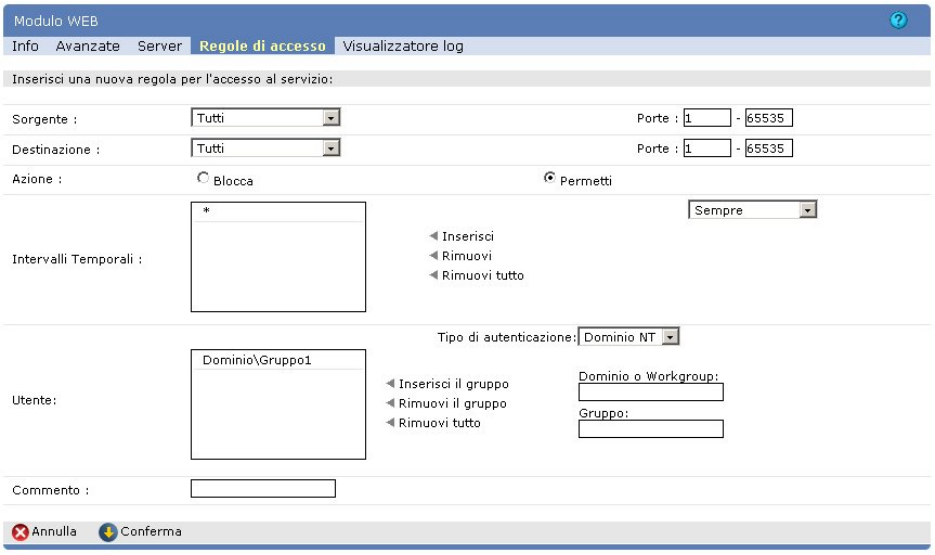


3. Salvare la configurazione con il tasto "Salva" e riavviare il modulo attraverso la sezione Info.

Come posso consentire la navigazione solo a certi utenti autenticati?

1. Dal configuratore premere su Moduli dal frame in alto e Modulo WEB dal menu sulla sinistra dell'interfaccia e poi Regole di accesso nella finestra principale.
2. Premere su Rimuovi tutto per cancellare la configurazione corrente ed iniziare la policy aziendale ex−novo. Confermare poi la selezione.

3. Premere su Inserisci sopra per inserire una nuova regola.
4. Nella nuova finestra, lasciare i valori di default per i campi "Sorgente" e "Destinazione" e il valore "Permetti" sul campo "Azione". Gli utenti a cui permettere la navigazione possono essere scelti da un dominio NT, un dominio Active Directory, un workgroup oppure mediante un file di testo che indica username e password degli utenti da autenticare. Si consiglia di consultare il manuale per avere maggiori informazioni. Premere poi su Conferma.

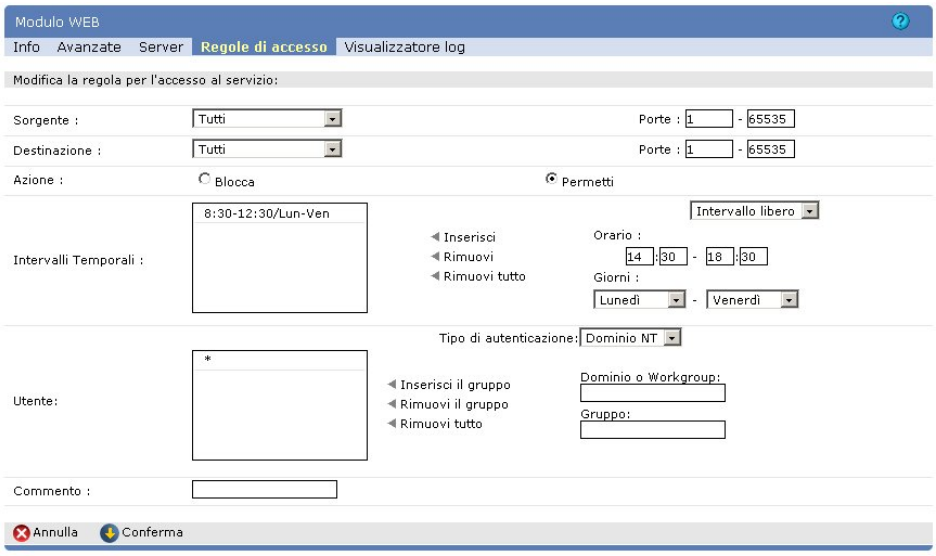


5. Riavviare il modulo dalla sezione Info.

Come posso vincolare la navigazione solo in certi orari?

1. Dal configuratore premere su Moduli in alto e poi su Modulo WEB dal menu sulla sinistra dell'interfaccia e poi Regole di accesso nella finestra principale.
2. Premere su Rimuovi tutto per cancellare la configurazione corrente ed iniziare la policy aziendale ex–novo. Confermare poi la selezione.

3. Premere su Inserisci sopra per inserire una nuova regola.
4. Nella nuova finestra, lasciare i valori di default per i campi "Sorgente" e "Destinazione" e il valore "Permetti" sul campo "Azione". Poi nella riga "Intervalli Temporali" selezionare sulla destra "Intervallo libero". Nel form che appare selezionare gli intervalli temporali in cui attivare la regola. È possibile utilizzare solo l'orario e questo verrà applicato a tutti i giorni, oppure vincolare l'orario a determinati giorni o intervalli giornalieri. L'inserimento avviene definendo l'intervallo nei form a destra e poi premendo sul tasto centrale "Inserisci". Premere poi su Conferma.



5. Riavviare il modulo dalla sezione Info.

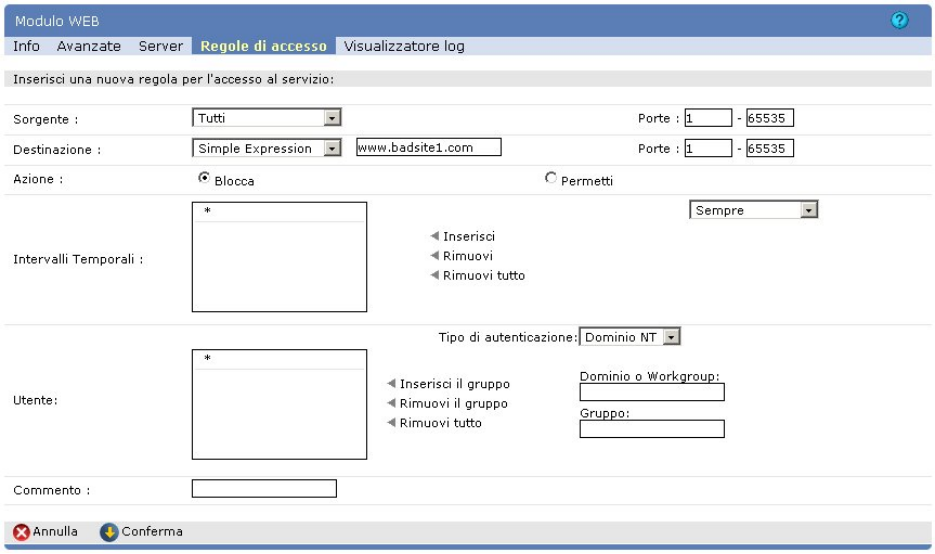
Come posso bloccare la navigazione verso certi siti?

Per bloccare la navigazione verso determinati siti si possono usare due diverse soluzioni. La prima prevede di creare una regola esplicita per ogni sito che si intende bloccare, una soluzione di questo tipo è sicuramente semplice e rapida ma è onerosa da applicare quando i siti da bloccare sono molti. La seconda prevede di creare una lista di siti e di utilizzare tale lista nella categorizzazione, questo permette una gestione ottimale anche di un elevato numero di siti.

Vediamo la prima soluzione, la creazione di una regola per sito.

1. Dal configuratore premere su "Moduli" in alto e poi su "Modulo WEB" dal menu sulla sinistra dell'interfaccia e poi "Regole di accesso" nella finestra principale.
2. Premere su "Rimuovi tutto" per cancellare la configurazione corrente ed iniziare la policy aziendale ex−novo. Confermare poi l'azione.

3. Premere su "Inserisci sopra" per inserire una nuova regola.
4. Nella nuova finestra, se si desidera applicare questo vincolo a tutti gli host locali lasciare nel campo "Sorgente" il valore "Tutti", altrimenti indicare mediante indirizzo IP o nome, le macchine a cui applicare questo vincolo. Nel campo "Destinazione" scegliere "Indirizzo IP" se si conosce l'indirizzo IP del sito che si vuole bloccare, "Simple Expression" se invece si conosce il nome. Premere poi su "Conferma".

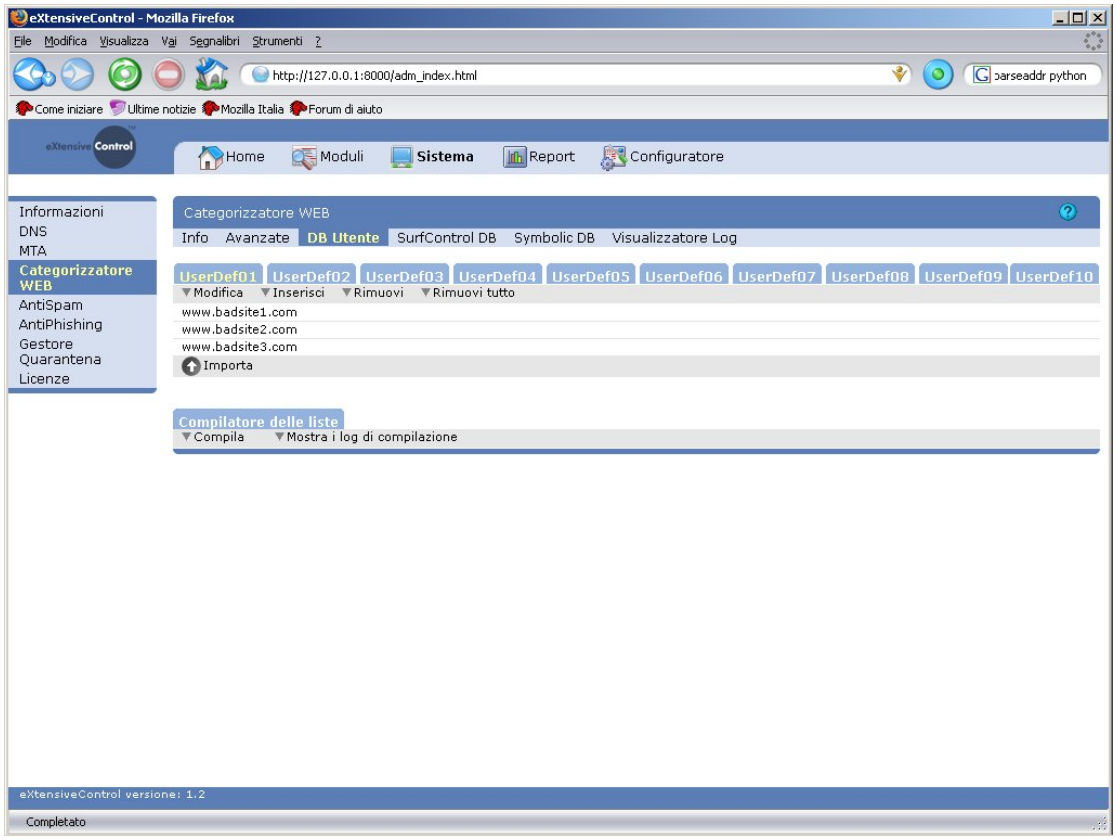


5. Ripetere i due passi precedenti tante volte quanti sono i siti da bloccare.
6. Premere su "Inserisci sotto", nella finestra di definizione scegliere l'azione "Permetti" lasciando ogni altro valore di default e poi "Conferma". Le regole di accesso saranno:

7. Riavviare il modulo dalla sezione "Info".

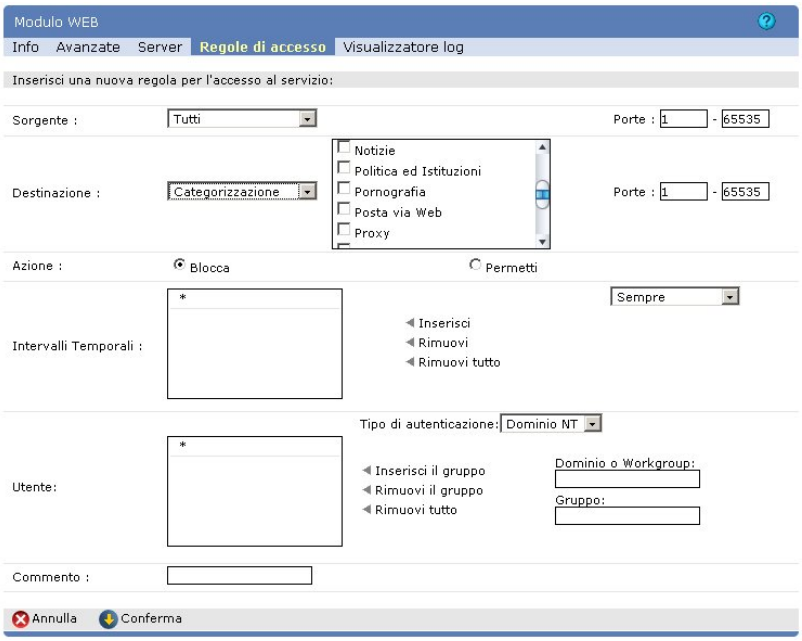
Qualora i siti da inserire fossero molti è opportuno optare per questa seconda soluzione.

1. Dal configuratore andare su "Sistema" nel frame in alto, poi "Categorizzatore WEB" nel menu a sinistra. Scegliere poi la sottosezione "DB utenti".



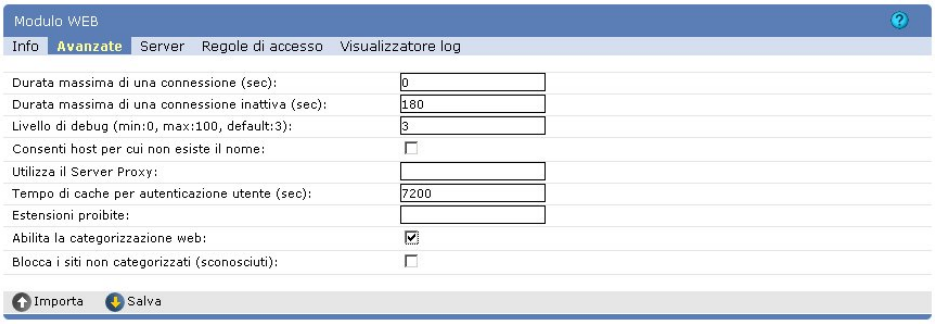
2. Scegliere una delle 10 liste disponibili, ad esempio "UserDef01", ed inserire in essa tutti i siti da bloccare mediante il tasto "Inserisci".
3. Una volta inseriti tutti i siti è necessario compilare il db utente mediante il tasto "Compila".
4. Riavviare il servizio di categorizzazione web dalla sottosezione "Info".
5. Premere nel frame in alto su "Moduli", poi dal menu a sinistra "Modulo WEB". Scegliere poi la sottosezione "Regole di accesso".
6. Premere su "Rimuovi tutto" per cancellare la configurazione corrente ed iniziare la policy aziendale ex–novo. Confermare poi la selezione.

7. Premere su "Inserisci sopra" per inserire una nuova regola.
8. Nella nuova finestra, se si desidera applicare questo vincolo a tutti gli host locali lasciare nel campo "Sorgente" il valore "Tutti", altrimenti indicare mediante indirizzo IP o nome, le macchine a cui applicare questo vincolo. Nel campo "Destinazione" scegliere "Categorizzazione" e nella finestra che apparirà selezionare la categoria "UserDef01". Nel campo "Azione" mettere "Blocca". Premere poi su "Conferma".



9. Creare poi una regola in ultima posizione che permetta tutto. Premere su "Inserisci sotto", nella finestra di definizione scegliere l'azione "Permetti" lasciando il resto invariato e poi "Conferma".

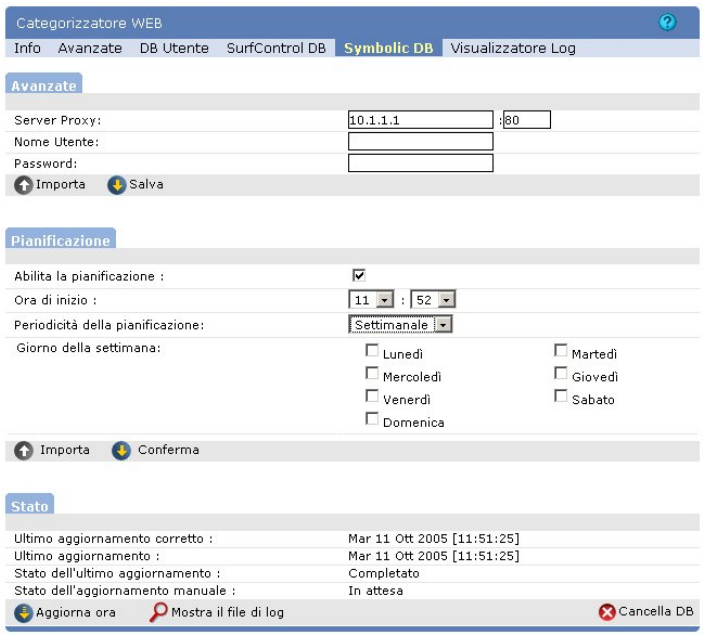
10. Premere su "Avanzate" e selezionare la voce "Abilita la categorizzazione web", poi cliccare su "Salva".



11. Riavviare il modulo andando su "Info" e poi "Riavvia".

Come posso aggiornare il database dei siti web in modo automatico?

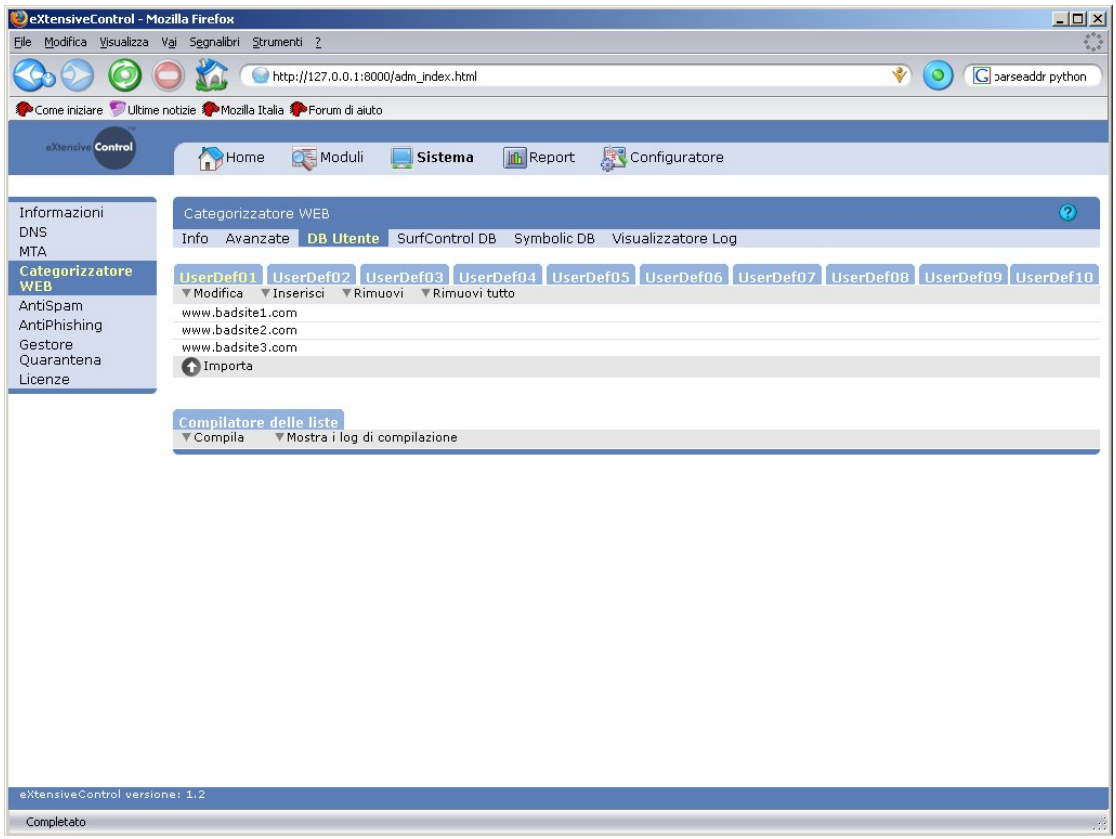
1. Dal configuratore andare su "Sistema" nel frame in alto, poi "Categorizzatore WEB" nel menu a sinistra. Scegliere poi la sottosezione "Symbolic DB" o "SurfControl DB" a seconda del database che si vuole aggiornare. L'interfaccia di configurazione sarà la medesima in entrambi i casi.



2. Se eXtensiveControl® si trova dietro ad un firewall di tipo proxy indicare nella sezione "Avanzate" l'indirizzo e la porta di ascolto del firewall e l'eventuale username e password da utilizzare. Premere "Salva".
3. Nella sezione "Pianificazione" selezionare il flag "Abilita la pianificazione" e definisci la periodicità e l'ora dell'esecuzione del download nei form sottostanti.Premere su "Conferma".

Come posso creare delle categorie personali?

1. Dal configuratore andare su "Sistema" nel frame in alto, poi "Categorizzatore WEB" nel menu a sinistra. Scegliere poi la sottosezione "DB utenti".



2. Scegliere una delle 10 liste disponibili, ed inserire in essa tutti i siti che si vogliono riconoscere in

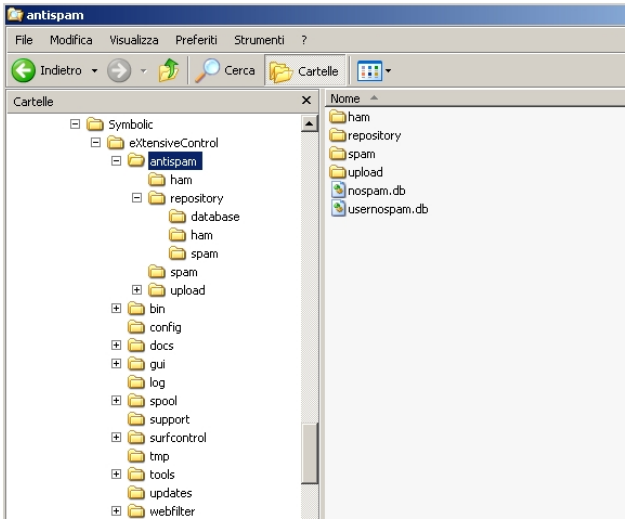
quella categoria mediante il tasto "Inserisci".

3. Una volta inseriti tutti i siti è necessario compilare il db utente mediante il tasto "Compila".
4. Riavviare il servizio di categorizzazione web dalla sottosezione "Info".
5. Fatto questo le liste definite possono essere utilizate nelle regole di accesso che fanno uso della categorizzazione, come se la lista fosse una qualunque categoria del db dei siti.

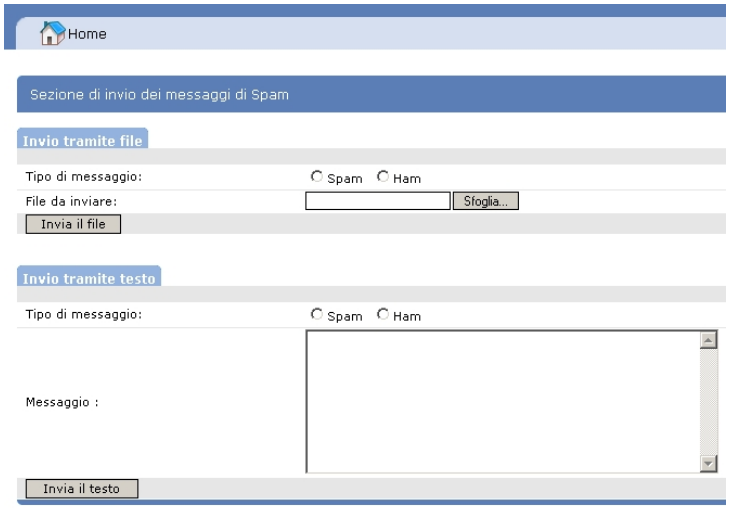
Capitolo 4. Gestione dello SPAM attraverso eXtensiveControl®

Come posso inserire i miei campioni di SPAM?

Esistono vari sistemi per inserire nuovi campioni di HAM e SPAM nel database, a seconda se siete l'amministratore di sistema o un utente, se avete la possibilità di operare direttamente sulla macchina su cui è installato il prodotto oppure se state operando da remoto.

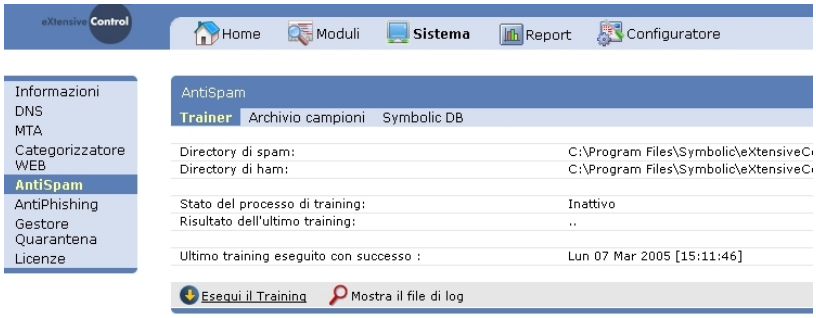


Esistono due cartelle HAM e SPAM nella sottocartella di installazione ANTISPAM (vedi figura sopra). In queste cartelle possono essere copiati direttamente i messaggi in formato ASCII che si vuole far elaborare al motore antispam. Una volta effettuato il training questi messaggi vengono automaticamente mossi nelle sottocartelle REPOSITORY/HAM e REPOSITORY/SPAM (vedi figura sopra).



In alternativa è possibile collegarsi con un web browser alla macchina di eXtensiveControl® ed effettuare singoli upload di campioni tramite la sezione "Inserimento SPAM".

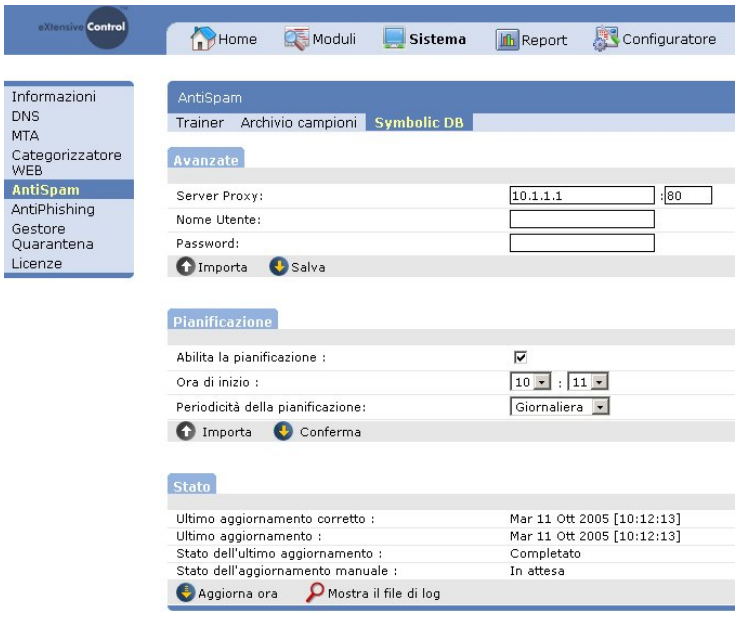
Per default ogni singolo upload deve essere verificato e confermato dall'amministratore prima che questo sia disponibile per il training. eXtensiveControl® può essere configurato in modo da rendere queste operazioni il più semplici ed automatiche possibili, per ulteriori informazioni si consiglia di consultare il manuale del prodotto.



In entrambi i casi, una volta che il campione arriva nelle opportune cartelle di raccolta è necessario effettuare il training del sistema e riavviare il proxy opportuno (POP3, SMTP o entrambi a seconda della configurazione allestita). Si consiglia di vedere il manuale del prodotto per avere i dettagli su come effettuare ciascuna di queste operazioni.

Come posso aggiornare in modo automatico il database di spam di Symbolic

1. Dal configuratore andare su "Sistema" nel frame in alto, poi "AntiSpam" nel menu a sinistra. Scegliere poi la sottosezione "Symbolic DB".

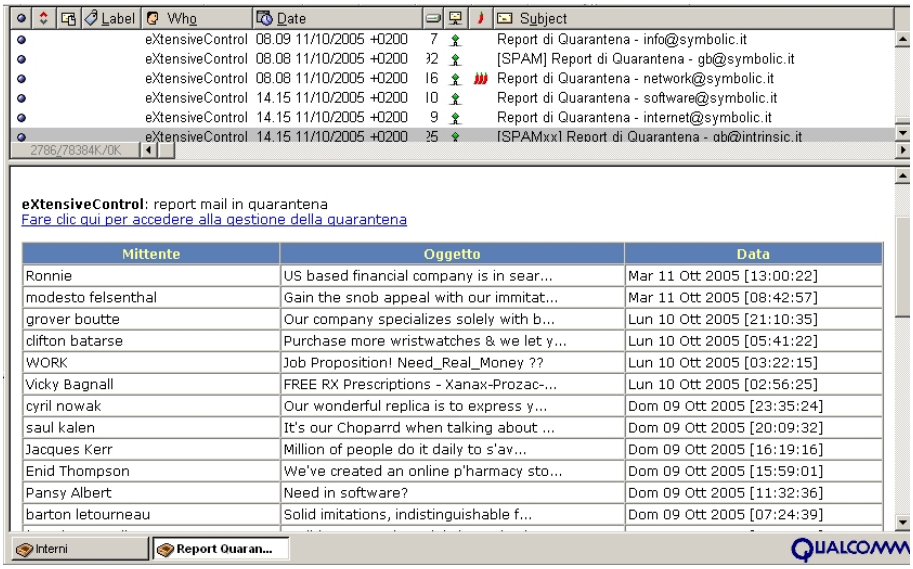


2. Se eXtensiveControl® si trova dietro ad un firewall di tipo proxy indicare nella sezione "Avanzate" l'indirizzo e la porta di ascolto del firewall e l'eventuale username e password da utilizzare. Premere "Salva".

3. Nella sezione "Pianificazione" selezionare il flag "Abilita la pianificazione" e definisci la periodicità e l'ora dell'esecuzione del download nei form sottostanti. Premere su "Conferma".

Cos'è e come si usa lo User Spam Management

Lo User Spam Management (USM) è una tabella riepilogativa che viene inviata ai singoli utenti per tenerli informati di quali messaggi sono stati messi in quarantena perchè considerati SPAM.



È possibile previo opportuna configurazione del server, decidere quali utenti includere e/o escludere dalla lista di chi ricevera l'USM ed anche inoltrare tale tabella ad utenti diversi dal destinatario prescelto (se ad esempio quest'ultimo è assente e la sua posta è gestita da una altra persona). In questo modo risulta comodo anche gestire quegli indirizzi collettivi (es. support, info, sales, ecc.) delegandone il controllo a una singola persona o ad un determinato gruppo di persone.

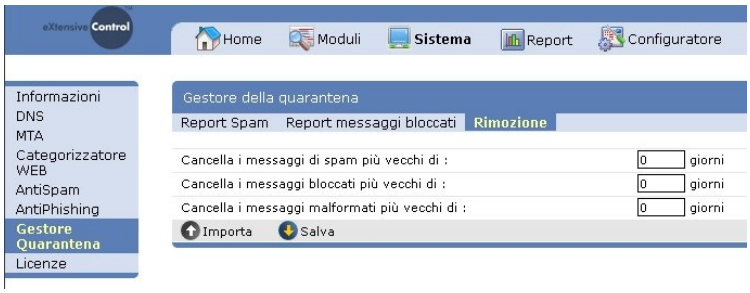
La tabella offre un link attraverso il quale l'utente può collegarsi al server e visualizzare, cancellare o rilasciare i messaggi quarantenati. Quest'ultimo potrà comunque agire solo sui propri messaggi senza poter accedere alle quarantene degli altri utenti.

Questa reportistica è disponibile anche per i messaggi bloccati perchè virati o in violazione delle politiche aziendali.

Si consiglia di vedere il manuale utente per maggiori dettagli.

Come posso rimuovere in modo automatico i messaggi dalla quarantena?

1. Dal configuratore andare su "Sistema" nel frame in alto, poi "Gestore Quarantena" nel menu a sinistra. Scegliere poi la sottosezione "Rimozione".



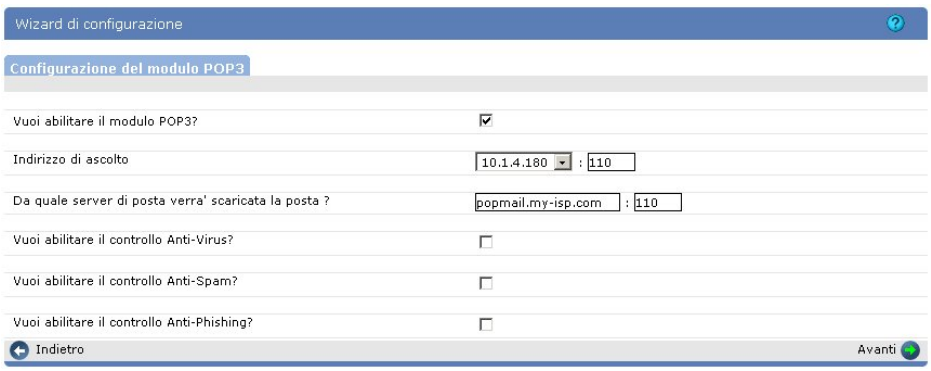
2. A questo punto è possibile impostare il tempo (in giorni) di mantenimento dei messaggi di spam, quelli bloccati dall'antivirus e quelli malformati (cioè che sono stati bloccati per altri motivi rispetto allo spam e al rilevamento di allegati infetti, tipicamente perchè non rispettano lo standard atteso). Poi premere su "Salva".

Capitolo 5. Configurazione per la gestione della posta elettronica

Come posso scaricare la posta da un server di posta esterno?

Per scaricare la posta da un server di posta esterno è necessario configurare il "Modulo POP3", il modo più semplice per farlo è attraverso il "Wizard di configurazione". L'utilizzo del wizard comporta la cancellazione di una eventuale configurazione preesistente.

1. Dalla schermata principale premere su "Wizard di configurazione" e poi autenticarsi con un utente avente i diritti di configurazione (ad esempio Admin).
2. Dalla schermata iniziale premere su "Avanti" e poi nuovamente su "Avanti".
3. Nella sezione dedicata al "Modulo POP3" selezionare "Vuoi abilitare il modulo POP3?" facendo apparire gli altri form di configurazione.
4. Indicare in "Indirizzo di ascolto" l'indirizzo IP e la porta su cui si porrà in ascolto il modulo. Si consiglia di mantenere i valori di default a meno che la coppia IP–porta non sia già in uso. Nella voce "Da quale server di posta verrà scaricata la posta?" indicare il mail server da contattare per il download, che nel caso specifico sarà quello del provider che fornisce il servizio di posta elettronica. Nelle ultime righe sono riportati tre checkbox per l'attivazione del controllo Anti–Virus, Anti–Spam ed Anti–Phishing. Poi premere su "Avanti".

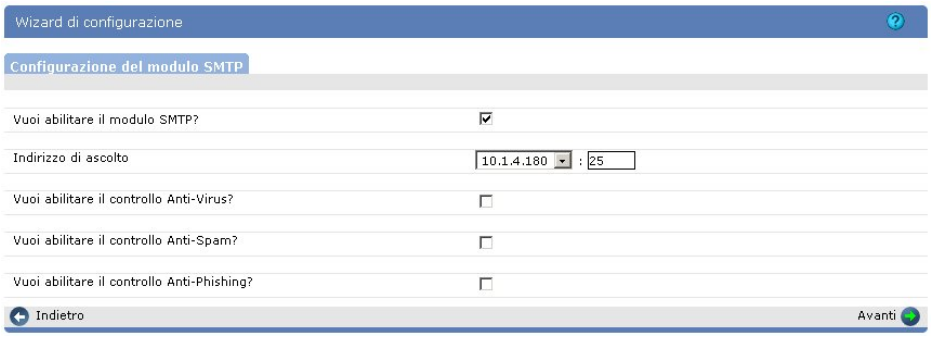


5. Premere "Avanti" fino al completamento del Wizard e poi "Finito".
6. Come detto ne la sezione chiamata «Gestione della posta con server di posta esterno» è necessario configurare il firewall per consentire l'uscita del protocollo POP3 solo dalla macchina su cui è installato eXtensiveControl® e configurare gli account dei client di posta per utilizzare eXtensiveControl® come server POP3 di Incoming.

Come posso ricevere la posta con un mail server interno?

Per fare in modo che tutta la posta in ingresso diretta al mail server aziendale venga controllata da eXtensiveControl®, è necessario configurare il "Modulo SMTP" ed il modo più semplice per farlo è attraverso il "Wizard di configurazione". Utilizzando il wizard una eventuale configurazione preesistente verrà sovrascritta.

1. Dalla schermata principale premere su "Wizard di configurazione" e poi autenticarsi con un utente avente i diritti di configurazione (ad esempio Admin).
2. Dalla schermata iniziale premere su "Avanti" fino al raggiungimento della sezione di configurazione del "Modulo SMTP".
3. Nella sezione dedicata al "Modulo SMTP" selezionare "Vuoi abilitare il modulo SMTP?" facendo apparire gli altri form di configurazione.
4. Indicare in "Indirizzo di ascolto" l'indirizzo IP e la porta su cui si porrà in ascolto il modulo. Si consiglia di mantenere i valori di default a meno che la coppia IP–porta non sia già in uso. Nelle ultime righe sono riportati tre checkbox per l'attivazione del controllo Anti–Virus, Anti–Spam ed Anti–Phishing. Poi premere su "Avanti".



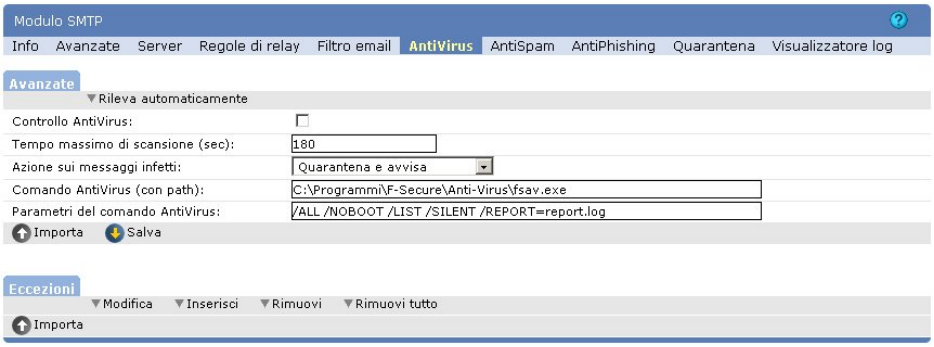
5. Nella sezione dedicata al "Modulo MTA" selezionare "Vuoi abilitare il modulo MTA?" facendo apparire gli altri form di configurazione.
6. La voce "Mail server per l'invio della posta" contiene il mail server da utilizzare come Relay, questo sarà l'indirizzo a cui verranno inviate tutte le mail non dirette verso il dominio interno e quindi da indirizzare verso il mondo esterno. Il mail server da utilizzare in generale in questo form è quello del provider che fornisce la connettività. Nella tabella sotto si dovranno riportare i domini interni aziendali e a lato il server di posta preposto alla gestione dello stesso.

7. Premere "Avanti" fino al completamento del Wizard e poi "Finito".

8. Come ultima cosa è necesario configurare il firewall in modo tale che le mail in ingresso vengano inviate ad eXtensiveControl® e non più al mail server aziendale.

Come posso abilitare il controllo AntiVirus?

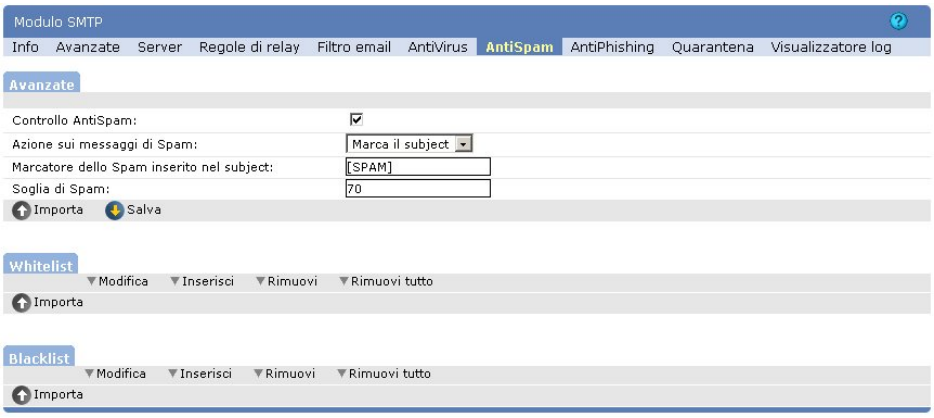
1. Dal configuratore premere su "Moduli" dal frame in alto e poi "Modulo POP3/SMTP" (a seconda del modulo per cui si vuole attivare il controllo) dal menu sulla sinistra dell'interfaccia e poi "AntiVirus" nella finestra principale.
2. Selezionare "Controllo AntiVirus" se è installato un antivirus supportato il path di installazione verrà rilevato automaticamente e saranno anche impostati i parametri di scansioni di default. Utilizzando un antivirus non supportato sarà necessario inserire manualmente il percorso in cui il programma ` installato e i parametri necessari al corretto funzionamento. Nel "Modulo SMTP" è possibile scegliere l'azione da intraprendere in caso di messaggio virato.



3. Riavviare il modulo dalla sezione "Info".

Come posso abilitare il controllo AntiSpam?

1. Dal configuratore premere su "Moduli" dal frame in alto e poi "Modulo POP3/SMTP" (a seconda del modulo per cui si vuole attivare il controllo) dal menu sulla sinistra dell'interfaccia e poi "AntiSpam" nella finestra principale.
2. Selezionare "Controllo AntiSpam". Il form relativo al marcatore permette di definire il tag da inserire all'interno dei subject delle mail di spam. Nel "Modulo SMTP" è possibile scegliere di mettere in quarantena o eliminare il messaggio oltre che a taggare il soggetto.



3. Riavviare il modulo dalla sezione "Info".

Come posso abilitare il controllo AntiPhishing?

1. Dal configuratore premere su "Moduli" dal frame in alto e poi "Modulo POP3/SMTP" (a seconda del modulo per cui si vuole attivare il controllo) dal menu sulla sinistra dell'interfaccia e poi

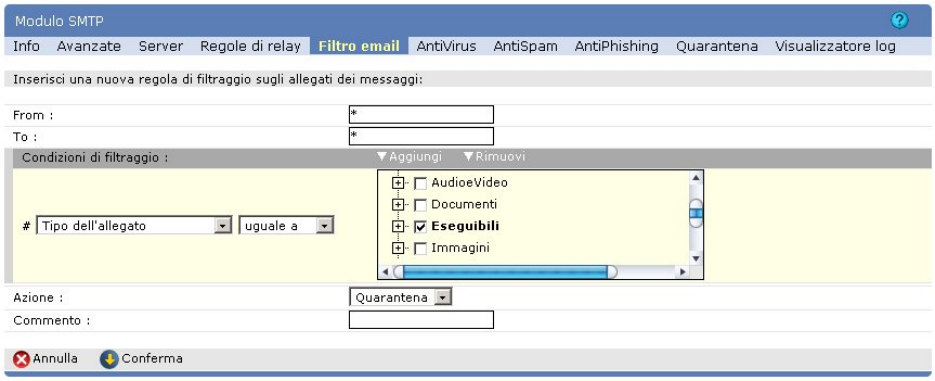
"AntiPhishing" nella finestra principale.

2. Selezionare "Controllo AntiPhishing". Il form relativo al marcatore permette di definire il tag da inserire all'interno dei subject delle mail di phishing. Nel "Modulo SMTP" è possibile scegliere di mettere in quarantena o eliminare il messaggio oltre che a taggare il soggetto.

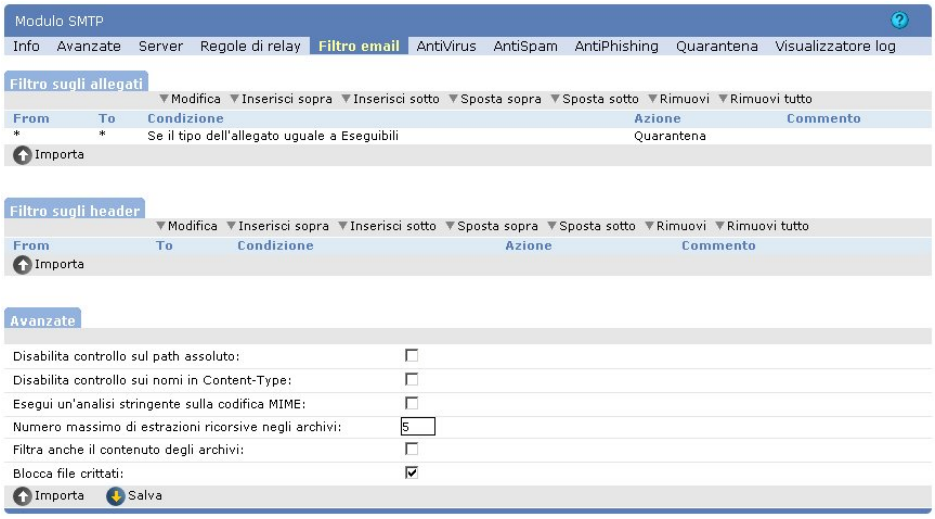
3. Riavviare il modulo dalla sezione "Info".

Come posso bloccare i messaggi con eseguibili come allegato?

1. Dal configuratore premere su "Moduli" dal frame in alto e poi "Modulo POP3/SMTP" (a seconda del modulo per cui si vuole attivare il controllo) dal menu sulla sinistra dell'interfaccia e poi "Filtro Email" nella finestra principale.
2. Dalla tabella "Filtro sugli allegati" premere su "Inserisci sopra".
3. Dalla schermata di configurazione della regola di filtraggio premere su "Aggiungi" e poi nella nuova riga che apparirà scegliere "Tipo dell'allegato". Nel frame selezionare "Eseguibili" e poi premere su "Conferma" lasciando ogni altro campo al valore di default.



4. La tabella "Filtro sugli allegati" avrà quindi una sola regola.



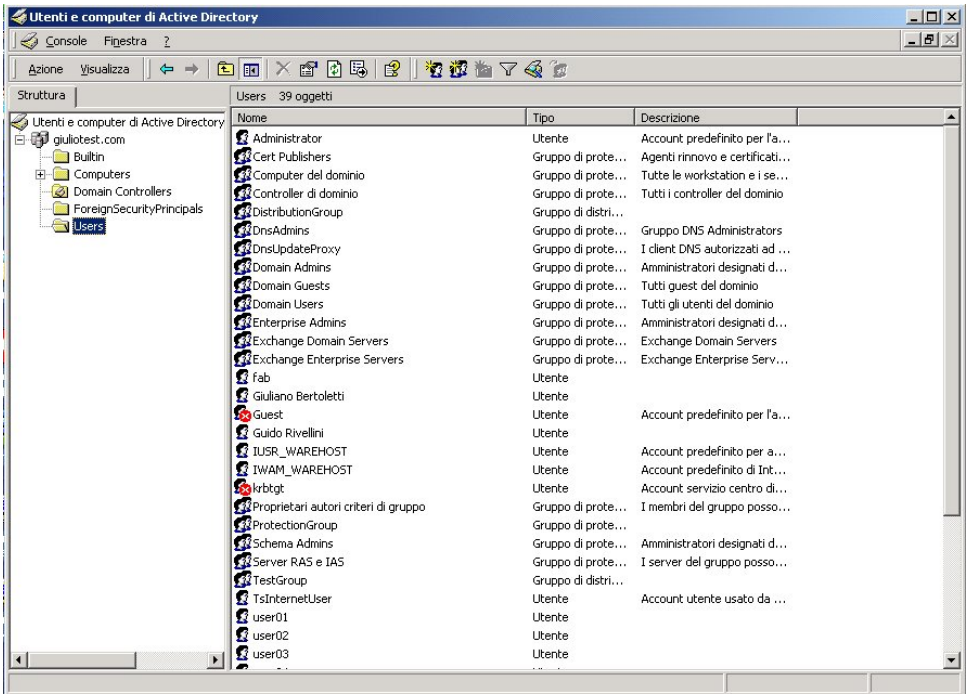
5. Riavviare il modulo dalla sezione "Info".

Per un ulteriore approfondimento sulle regole di filtraggio si consiglia di consultare il manuale.

Capitolo 6. Active Directory

Cos'è Active Directory ?

Active Directory è un database integrato nei server Windows 2000 e Windows 2003 che fungono da domain controller e consente di catalogare e gestire in modo centralizzato risorse di vario genere come: utenti, gruppi di lavoro, stampanti, cartelle condivise, ecc. La struttura del database è di tipo gerarchico, con contenitori che contengono oggetti e altri contenitori.



A cosa serve collegare eXtensiveControl® ad Active Directory

Solitamente in un dominio Windows 2000/2003 l'amministratore gestisce attraverso Active Directory le varie risorse a disposizione. Fornendo le opportune credenziali di amministratore di dominio, eXtensiveControl® può accedere (in sola lettura) ad alcune di queste risorse.

Per esempio eXtensiveControl® può sfruttare il database Active Directory per controllare le credenziali di quegli utenti che richiedono il servizio di navigazione WEB.

Inoltre, se si utilizza un server di posta Microsoft Exchange, è possibile, sempre attraverso il collegamento ad Active Directory, impostare un filtro che rifiuti le e–mail destinate ad utenti del dominio inesistenti. In pratica si evita di sovraccaricare il server di posta eliminando a monte i messaggi comunque destinati ad essere respinti.

Di cosa ho bisogno per collegare eXtensiveControl® ad un dominio Active Directory

Sono necessarie le credenziali (username e password) di un utente abilitato ad effettuare query sul domain controller e di una connessione di rete che consenta di raggiungere quest'ultimo.

Quali sono gli scenari tipici di funzionamento con Active Directory?

Se si utilizza eXtensiveControl® per gestire la navigazione WEB ed eventualmente anche la posta elettronica, la macchina viene tipicamente installata sulla rete locale. L'autenticazione WEB necessita del funzionamento del sottosistema NetBios per la comunicazione con il domain controller ed è consigliabile non interporre firewall fra l'host su cui è installato eXtensiveControl® e il domain controller stesso. Viene anche impiegata la porta 389 per effettuare query LDAP sempre sul domain controller e per gestire il filtro su Exchange.

Nel caso si utilizzi invece solo la posta elettronica, oltre all'installazione sulla rete interna descritta prima è possibile allestire una configurazione in DMZ con la macchina che ospita eXtensiveControl® che sta su quest'ultima. In tal caso il firewall dovrà permettere il passaggio della porta LDAP (389) e del DNS (per risolvere i nomi), oltre ovviamente alla porta SMTP (25) per il transito dei messaggi.

Come funziona il filtro Exchange?

Il filtro Exchange è stato pensato per bloccare i messaggi diretti ad utenti non esistenti prima che questi arrivino sul server di posta.

Quando arriva un messaggio ad un utente del dominio il programma controlla che tale utente esista realmente nella lista presente in Active Directory prima di passare il messaggio al server Exchange. Se tale utente non esiste il messaggio viene respinto da eXtensiveControl®

È possibile utilizzare un filtro di questo tipo con altri server di posta?

Per ora no, in quanto al momento solo Exchange altera lo schema di Active Directory in modo da inserire nel database gli utenti aventi una casella di posta elettronica.

E' tuttavia possibile, se il server lo supporta, estrarre in qualche modo gli utenti e memorizzarli su un file esterno che il proxy SMTP di eXtensiveControl® legge all'avvio. L'operazione di creazione ed aggiornamento del suddetto file non avviene in modo automatico ed è lasciata all'utente.